

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

Case No. 5:22-CR-00178-M

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICO AARON LOWERS,

Defendant.

ORDER

This matter comes before the court on Defendant's motion to suppress [DE 40]. The motion is fully briefed, DE 51; DE 55, and the parties stipulated to the material facts, DE 57; DE 58, obviating the need for a hearing. Defendant's motion presents a straightforward legal question, albeit in a burgeoning and undefined area of Fourth Amendment jurisprudence: does a law enforcement officer's warrantless inspection of a digital file provided to the officer and identified as a hash value match to child pornography by a private internet service provider (in this case, Google) constitute an unreasonable search in violation of the Fourth Amendment? The court finds that it does not. Accordingly, and for the reasons that follow, the motion to suppress is DENIED.

I. Factual Background¹

Defendant is charged with transporting and possessing child pornography in violation of 18 U.S.C. § 2252. DE 1 at 1-2. The investigation into Defendant's conduct began in 2019. *See* DE 40 at 1. On September 23, 2019, Google made a CyberTip Report (the "Report") to the National Center for Missing and Exploited Children ("NCMEC"). *Id.* That Report indicated that

¹ Because the parties stipulated to the material facts, the court considers as true the factual statements made in the motion, the United States' response, and Defendant's reply. Even so, the court will cite to corroborating documentary evidence where it is available.

a Google user had uploaded 156 images of “Apparent Child Pornography” onto a cloud-based Google drive. *Id.* at 1-2; *see also* DE 40-1 at 2, 4-5; DE 51 at 1-2.

Of those 156 images, a Google employee viewed 31 of them and identified them as child pornography immediately prior to generation and transmission of the Report. *Id.* at 2. The remaining 125 images were included in the Report as apparent child pornography because Google identified those images as a hash value match to images previously identified by Google employees as child pornography. *Id.* at 3; *see also* DE 51 at 2. “A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file.” Fed. R. Evid. 902 advisory committee note to 2017 amendment; *see also United States v. Wilson*, 13 F.4th 961, 964 (9th Cir. 2021); *United States v. Miller*, 982 F.3d 412, 418 (6th Cir. 2020); *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018) (all discussing Google’s hash value system).

Fair consideration of the motion to suppress requires a baseline understanding of hash values and hash searches. “Hashing is a powerful and pervasive technique [in which one] take[s] a large amount of data, such as a file . . . , and use[s] a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data.” Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38 (2005). Because an algorithm that generates hash values produces a unique numerical identifier for each file, a subsequent hash match between two files establishes a virtual certainty that the two files are the same; “[i]f two nonidentical files are inputted into [a] hash program, the computer will output different results.” Orin S. Kerr, *Searches and Seizures in A Digital World*, 119 HARV. L. REV. 531, 541 (2005); *see also id.* at 546 (“If there is a match between the hash of a known file in a database and a file located in [a] computer being searched, an analyst can be confident that he has

identified a particular file without actually opening or looking at it.”); Salgado, 119 HARV. L. REV. F. at 46 (“Hash-based file detection works extraordinarily well in identifying *only those files that are exact matches*”) (emphasis added). As for a hash search’s capacity to identify contraband, “hash searches are like dog sniffs but even better.” Dennis Martin, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 717 (2018); *see also* Rebekah A. Branham, *Hash It Out: Fourth Amendment Protection of Electronically Stored Child Exploitation*, 53 AKRON L. REV. 217, 219 (2019) (citing evidence that the chance of two different files sharing the same hash value “is less than one in one billion”).

If a hash search has any shortcomings as it relates to identifying contraband, it is that a hash search may be *too* precise. To that point, if a single pixel within an image has been altered, the image will be represented by a hash value distinct from its unaltered version. *See* Branham, 53 AKRON L. REV. at 237; *United States v. Keith*, 980 F. Supp. 2d 33, 36–37 (D. Mass. 2013). Thus, an image may be (for all intents and purposes) the same image as one already confirmed to contain child pornography, but possess a different hash value due to minor modification of a single pixel within that image. The modified image of child pornography could then evade identification through a hash search. But, for present purposes, suffice it to say that if two images share the same hash value, they are “identical, bit-for-bit.” Salgado, 119 HARV. L. REV. F. at 39.

“Google uses a proprietary hashing technology to detect apparent [child pornography].” DE 40-2 at 3. Google has no legal obligation to monitor its systems for the presence of child pornography, *see* 18 U.S.C. § 2258A(f)(1) – (3), but it does so for reputational and business reasons, *see* DE 40-2 at 2-3. To that end, Google users must agree that they will not use Google’s services to upload, receive, or distribute any child pornography, and Google’s privacy policy informs its users that Google may monitor user activity to detect illegal content. *See id.* at 2.

Although Google is under no obligation to engage in such monitoring, once Google detects the presence of child pornography, it is required to make a report to NCMEC. *See* 18 U.S.C. § 2258A(a)(1).

Google's technology is deployed in a process as follows: Google trains certain employees to identify child pornography. DE 40-2 at 3. An employee then views a file suspected to be child pornography. *See id.* If the employee concludes that the image constitutes child pornography, the image is "given a digital fingerprint," referred to as a hash value. *Id.* Google stores these hash values on an internal system. *Id.* Google then compares the hash values to images later uploaded to Google's systems and services. *Id.* If a later-uploaded image contains a hash value that matches the hash value of a previously reviewed image of child pornography, Google reports the later-uploaded image to NCMEC as child pornography. *Id.* at 2-3. The later-uploaded image may or may not be visually reviewed by a Google employee. *Id.* at 3.

In the present case, as noted, a Google employee visually inspected 31 of the 156 images and identified them as child pornography immediately prior to transmission of the Report to NCMEC. *See* DE 40-1. NCMEC, in turn, viewed the same 31 images. *See id.* at 42. Based on the IP address included in the report, and consistent with its own statutory obligations, NCMEC forwarded the Report to the Bedford County, Virginia Sheriff's Office for further investigation on October 29, 2019. DE 40-3 at 3; 18 U.S.C. § 2258A(c)(2).

Several months later, on April 16, 2020, an investigator in that office reviewed the Report. *See id.* at 2. He then obtained an administrative subpoena, the results of which linked the IP address to a subscriber in Chesapeake, Virginia. *Id.* On or about May 13, 2020, the investigator forwarded the Report to the Chesapeake Police Department. *Id.*

Shortly thereafter, a detective in the Chesapeake Police Department (“Detective Rider”) downloaded the Report. *Id.* at 4. Detective Rider then viewed at least 3 of the 156 images included in the Report. *Id.* The images viewed by Detective Rider were not among the 31 images that a Google employee had visually inspected prior to transmission of the Report, but rather were among the 125 hash value match images included in the Report. *See* DE 40 at 3.

After viewing those images, on May 27, 2020, Detective Rider applied for a search warrant for the Google account that had originally uploaded the images. DE 40-4 at 2. The warrant affidavit notes that the affiant reviewed the images in the Report. *Id.* at 5. The affidavit also includes a description of one of the images, although the description of that image does not match that of any of the three images previously described in Detective Rider’s report. *Compare id., with* DE 40-3 at 4.² The warrant return indicated that the Google account was created on September 20, 2019, and active for a span of only 30 minutes, during which time the user uploaded the 156 images to the Google drive. DE 40-3 at 4. The account was never accessed again. *Id.*

Further investigation into the IP address revealed that it was linked to a residence in Chesapeake owned by Defendant’s parents. *Id.* at 4-5. Detective Rider conducted surveillance at the residence from July to September 2020. *Id.* at 6. Then, in October 2020, Detective Rider sought and obtained a search warrant for the Chesapeake residence. *Id.* at 7. The warrant affidavit included descriptions of the three images Detective Rider viewed on or about May 13. *Compare id. at 4, with* DE 51-2 at 11.

Law enforcement seized 10 devices during execution of the search warrant on October 12, 2020. *Id.* No evidence of child pornography was located on any of those devices. *Id.* In addition, Defendant’s parents were interviewed while law enforcement executed the warrant. *Id.* They

² This discrepancy suggests that the detective viewed more than 3 of the 156 images, and may have viewed one or more of the 31 images viewed by the Google employee.

denied knowledge of any child pornography, but mentioned that their son, Defendant, had moved out of their house several months prior and relocated to Raleigh, North Carolina. *Id.* Defendant's parents provided law enforcement with Defendant's new address and phone number. *Id.* at 8.

Chesapeake PD then closed their case but forwarded the information they had collected to law enforcement in North Carolina, at which point Defendant became the subject of the investigation. *See id.*; *see also* DE 51 at 5. Law enforcement in North Carolina contacted Defendant, and asked whether they could interview him to discuss the search that occurred at his parents' home in Chesapeake. DE 51 at 5. Defendant agreed to participate in a voluntary interview. *Id.*

Defendant was interviewed by law enforcement on November 24, 2020. *Id.* He denied knowledge of the Google account or any child pornography. *Id.* at 5-6. At the conclusion of the interview, he gave law enforcement consent to examine his laptop computer and cellular phone. *Id.* at 6; *see also* DE 51-3 at 1.

In the days following that interview, law enforcement analyzed Defendant's devices and found four videos of child pornography on his phone that had previously been deleted. *Id.* at 6-7. They also found "child erotica" on his laptop and other sexual images in which it was difficult to ascertain the ages of the individuals. *Id.* at 7. Law enforcement then contacted Defendant and asked whether he would submit to another voluntary interview. *Id.* Defendant agreed, and the interview was scheduled for December 8, 2020. *Id.*

When Defendant arrived at the Raleigh police station for his second interview, he was reminded that the interview was voluntary and that he could leave at any time. *Id.* at 9. Defendant continued to deny any knowledge of child pornography. *Id.* Law enforcement then confronted Defendant with the videos they had recovered from his cell phone. *Id.* At that point, Defendant

admitted to downloading child pornography onto a flash drive in Virginia and bringing that flash drive with him when he moved to Raleigh. *Id.* He told officers that the flash drive was stored in a wooden box in his bedroom. *Id.* at 9-10.

Law enforcement had already sought and obtained a search warrant for Defendant's Raleigh apartment prior to his second interview. *Id.* at 8. They executed that warrant during the December 8 interview. *Id.* at 10. Two officers left the interview to participate in the search, and located the flash drive that Defendant had described. *Id.* The flash drive contained 264 images and 17 videos of child pornography. *Id.* Law enforcement also discovered a hard drive in Defendant's apartment that contained 764 images and 11 videos of child pornography. *Id.* at 11.

Defendant was federally indicted. *See* DE 1. Count One of the Indictment charges him with transporting child pornography, "[b]eginning on or about June 27, 2020, [and] continuing through on or about September 30, 2020." *Id.* at 1. Count 2 charges him with possessing child pornography "[o]n or about December 8, 2020," the day of the search warrant at his Raleigh apartment. *Id.* The charges do not relate to any conduct on September 20, 2019, the date on which the Google user uploaded 156 images of child pornography. *See id.* Defendant now moves to suppress "[a]ll evidence in this case," DE 40 at 1, on the grounds that the evidence is tainted by Detective Rider's review of three images in May 2020 that were not among the 31 images visually inspected by the Google employee prior to generation of the Report, *see generally id.*

II. Legal Standards

The Fourth Amendment protects against "unreasonable searches and seizures." U.S. Const. amend. IV. A search occurs when a government actor infringes upon a reasonable expectation of privacy. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also United States v. Jacobsen*, 466 U.S. 109, 113 (1984). On the other hand,

“[o]fficial conduct that does not compromise any legitimate interest in privacy is not a search subject to the Fourth Amendment.” *Illinois v. Caballes*, 543 U.S. 405, 408 (2005). Because an individual does not have a legitimate interest in possessing contraband, government conduct that reveals only the presence or absence of contraband does not constitute a search. *See id.*; *see also United States v. Pyne*, 175 F. App’x 639, 641 (4th Cir. 2006).

Where an individual does have a reasonable expectation of privacy, “a search conducted without a warrant issued upon probable cause is per se unreasonable, subject only to a few specifically established and well-delineated exceptions.” *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (internal quotation marks and ellipses omitted). One of those exceptions is the private search doctrine, which “is based on the principle that the Fourth Amendment does not protect against searches conducted by private individuals acting in a private capacity.” *United States v. Fall*, 955 F.3d 363, 370 (4th Cir. 2020). In that regard, “a private party may conduct a search that would be unconstitutional if conducted by the government.” *Wilson*, 13 F.4th at 967; *see also Burdeau v. McDowell*, 256 U.S. 465, 475 (1921) (explaining that Fourth Amendment “was not intended to be a limitation upon other than governmental agencies”). The justification underlying this exception is that when a private party collects evidence of criminality and subsequently presents that evidence to the police, the police need not “avert their eyes.” *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971).

The private search doctrine “is implicated when a private party conducts a search of private information and the government subsequently reviews that same information without first obtaining a search warrant.” *United States v. Bonds*, No. 5:21-CR-00043, 2021 WL 4782270, at *2 (W.D.N.C. Oct. 13, 2021). The critical inquiry, therefore, is whether the government “obtained information with respect to which the defendant’s expectation of privacy ha[d] not already been

frustrated.” *Reddick*, 900 F.3d at 638. In other words, when there is a “virtual certainty” that a government search will identify “nothing ... of significance” that the private search did not already reveal, the doctrine applies and no Fourth Amendment violation occurs. *Jacobsen*, 466 U.S. at 119.

In applying the private search doctrine to a government search of hash value matches of child pornography, the Courts of Appeals have reached varying results. *Compare Wilson*, 13 F.4th at 973 (concluding police search of hash match files exceeded Google’s search because viewing the images “substantively expanded the information available to law enforcement far beyond what the label alone conveyed”), *with Miller*, 982 F.3d at 429–30 (holding that police search of hash match files did not exceed Google’s search because there was a virtual certainty that police only viewed the same images that Google had already viewed), *and Reddick*, 900 F.3d at 639 (finding private search doctrine applied because police officer’s “opening [of] the file merely confirmed that the flagged file was indeed child pornography, as suspected”). Without authoritative guidance from the Fourth Circuit, this court’s analysis remains primarily guided by the standard set forth in *Jacobsen*: a government search does not exceed a private search when there is a “virtual certainty” that the government search would reveal “nothing ... of significance” that the private search did not already reveal. *Jacobsen*, 466 U.S. at 119.

Another exception to the warrant requirement is the good faith exception. *See United States v. Leon*, 468 U.S. 897, 922 (1984). The good faith exception reflects the principle that excluding evidence obtained from an unreasonable search or seizure “has always been [a] last resort, not [the] first impulse.” *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). The exception applies when a law enforcement officer acts in objectively reasonable reliance on a statute that authorizes the search. *Illinois v. Krull*, 480 U.S. 340, 358 (1987); *see also United States v.*

Ackerman, 804 F. App'x 900, 904–05 (10th Cir. 2020) (affirming denial of motion to suppress and finding good faith exception applied where NCMEC opened four files attached to email even though internet service provider had only identified one file as apparent child pornography); *United States v. Brillhart*, No. 2:22-CR-53, 2023 WL 3304278, at *8–9 (M.D. Fla. May 7, 2023) (applying good faith exception to police officer who “acted in reasonable reliance on Yahoo’s, Google’s, and NCMEC’s legal obligations to view the files she received”).

Although not a per se exception to the warrant requirement, a court considering a challenge to evidence obtained from a purportedly unlawful search must also consider attenuation. As the Supreme Court has explained, “a causal connection between information obtained through illicit [means] and the Government’s proof . . . may [] become so attenuated as to dissipate the taint.” *Nardone v. United States*, 308 U.S. 338, 341 (1939). In considering attenuation, “the [] apt question . . . is whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.” *Wong Sun v. United States*, 371 U.S. 471, 488 (1963) (internal quotation mark omitted). “That is, if police discover the evidence from a[] source independent from the illegal conduct, the evidence need not be excluded.” *United States v. Harris*, 175 F.3d 1017 (Table), 1999 WL 133134 at *2 (4th Cir. 1999). A defendant’s consent is often sufficient to “sever the connection between an unlawful act and the acquisition of additional evidence[, because] voluntary consent is the quintessential act of free will.” *United States v. Seidman*, 156 F.3d 542, 549 n.10 (4th Cir. 1998); *see also Schneekloth*, 412 U.S. at 243 (“there is nothing constitutionally suspect in a person’s voluntarily allowing a search”); *but see Brown v. Illinois*, 422 U.S. 590, 603 (1975) (holding that Miranda warnings issued shortly after illegal arrest were insufficient to render subsequent murder confession “a product of free will”).

Lastly, a word about process. Recall that a search subject to the Fourth Amendment only occurs when a government actor infringes upon a reasonable expectation of privacy. *See Katz*, 389 U.S. at 361. On a motion to suppress, “[t]he burden of showing a reasonable expectation of privacy in the area searched rests with the defendant.” *United States v. Gray*, 491 F.3d 138, 144 (4th Cir. 2007). Discharging this burden “normally embraces two discrete questions.” *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

First, the defendant must provide evidence demonstrating a subjective expectation of privacy in the area searched. *See id.* Courts “cannot just assume a subjective expectation of privacy.” *United States v. Ulbricht*, No. 14-CR-68, 2014 WL 5090039, at *13 (S.D.N.Y. Oct. 10, 2014), *aff’d*, 858 F.3d 71 (2d Cir. 2017). “But it is not enough that an individual have a subjective expectation of privacy.” *Gray*, 491 F.3d at 145. That subjective expectation of privacy must be “one that society is prepared to recognize as ‘reasonable.’” *Smith*, 442 U.S. at 740 (quoting *Katz*, 389 U.S. at 361). A defendant’s subjective expectation of privacy must, therefore, be objectively reasonable. *See id.*

III. Analysis

Five independent (and independently sufficient) bases justify denying the motion to suppress. **First**, Defendant failed to meet his burden of production in demonstrating a reasonable expectation of privacy in his Google account. **Second**, Detective Rider’s inspection of images of apparent child pornography does not constitute a search within the meaning of the Fourth Amendment because Defendant cannot maintain a reasonable expectation of privacy in the possession of contraband. **Third**, Detective Rider’s review of the three images did not exceed Google’s search because there is a virtual certainty that his search would reveal nothing of significance that Google’s search did not already reveal. **Fourth**, even if Detective Rider’s search

was unlawful, the good faith exception applies. *Fifth*, and finally, Defendant's ultimate arrest and indictment is sufficiently attenuated from Detective Rider's visual inspection of the three images that, to the extent that search resulted in taint, subsequent intervening circumstances dispelled it.

First, Defendant has not established a reasonable expectation of privacy in the storage of child pornography in his Google account. Assuming Defendant possessed a subjective expectation of privacy in his Google account, he has not met his burden in showing that such an expectation would be objectively reasonable. To that point, Google users must agree that they will not use Google's services to upload any child pornography, and Google's privacy policy informs its users that Google may monitor user activity to detect illegal content. *See* DE 40-2 at 2. Those terms "limit[] Defendant's objectively reasonable expectation of privacy." *United States v. Ackerman*, 296 F. Supp. 3d 1267, 1272 (D. Kan. 2017) (holding that defendant had no reasonable expectation of privacy in his AOL account), *aff'd*, 804 F. App'x 900 (10th Cir. 2020). Defendant agreed to those terms of service when he created his Google account, but the motion to suppress neglects to grapple with the consequences of that acquiescence. *See* DE 40; *accord Carpenter v. United States*, 138 S. Ct. 2206, 2219 (2018) (reiterating that "an individual has a reduced expectation of privacy in information knowingly shared with another").

As several other district courts have concluded, "given the prohibitions and reservations of rights in [Google's terms of service and privacy policy], even for the CyberTips involving uploaded images and videos whose contents were not publicly available, a reasonable person would not have viewed files containing prohibited content as private. And Defendant has not submitted any evidence to the contrary." *United States v. Tennant*, No. 5:23-CR-79, 2023 WL 6978405, at *9 (N.D.N.Y. Oct. 10, 2023) (denying motion to suppress child pornography recovered in searches of defendant's social media accounts) (internal quotation marks omitted).

Put another way, “Google warned Defendant he risked being reported to law enforcement or NCMEC if [it] discovered that he sent, received, or distributed apparent child pornography. Even if Defendant believed that his [content was] private, society is not prepared to recognize that belief as reasonable given the Terms of Service.” *Brillhart*, 2023 WL 3304278, at *8 (denying motion to suppress evidence of child pornography recovered from defendant’s Yahoo and Google accounts). Accordingly, Defendant has not met his burden in demonstrating that any subjective expectation of privacy was objectively reasonable. *See Gray*, 491 F.3d at 144.³

Second, even if Defendant possessed a reasonable expectation of privacy in his Google account generally, he could not maintain a reasonable expectation of privacy in the 156 images of apparent child pornography extracted from that account by Google and turned over to law enforcement. The motion to suppress (at least implicitly) recognizes this distinction, by detailing that “law enforcement reviewed files from [Defendant’s] Google Drive account *after* the files were sent to NCMEC, and NCMEC . . . in turn created another copy of the files and sent them to local law enforcement in Virginia.” DE 40 at 10 (emphasis added). Therefore, the relevant constitutional question is whether Defendant retained a legitimate privacy interest in the files, not his account.

The court finds he did not. As recounted previously, Google trains its employees to identify apparent child pornography. DE 40-2 at 3. Once an image or video is identified as child pornography, it is given as hash value, which is compared to later-uploaded images. *See id.* Google’s hashing technology is “highly reliable—akin to the reliability of DNA.” *United States v. Miller*, No. 16-CR-47, 2017 WL 9325815, at *10 (E.D. Ky. May 19, 2017), *recommendation adopted*, No. 16-CR-47, 2017 WL 2705963 (E.D. Ky. June 23, 2017), *aff’d*, 982 F.3d 412 (6th

³ The court’s conclusion on this issue stems from a lack of evidence on Defendant’s part and is not intended to suggest any per se rule that an individual lacks a reasonable expectation of privacy in an online account.

Cir. 2020). One court found that “[t]he chance of two files coincidentally sharing the same hash value is 1 in 9,223,372,036,854,775,808.” *United States v. Dunning*, No. 7:15-CR-4, 2015 WL 13736169, at *2 (E.D. Ky. Oct. 1, 2015), *recommendation adopted*, No. 7:15-CR-4, 2015 WL 5999818 (E.D. Ky. Oct. 15, 2015), *aff’d*, 857 F.3d 342 (6th Cir. 2017). “That is 1 in 9.2 quintillion in case you were wondering.” *Miller*, 982 F.3d at 430; *accord United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011) (noting district court finding “that files with the same hash value have a 99.99 percent probability of being identical”). Notably, the motion to suppress does not challenge the reliability of either Google’s human review or its hashing technology.

As a result, when Google provided the Report to NCMEC (which in turn provided the Report to law enforcement), that Report contained 156 images of “Apparent Child Pornography.” DE 40-1 at 2. In this context, apparent means “obvious.” *Pearson v. Colvin*, 810 F.3d 204, 209 (4th Cir. 2015).⁴ And child pornography constitutes contraband. *United States v. Bosyk*, 933 F.3d 319, 326 (4th Cir. 2019). Ergo, Google provided law enforcement with 156 images that were obvious contraband. *See* DE 40-1. The motion to suppress does not argue otherwise.

Therefore, Detective Rider’s subsequent visual inspection of those images was not a search subject to the Fourth Amendment because he viewed obvious contraband, nothing more, and “governmental conduct that only reveals the possession of contraband compromises no legitimate privacy interest.” *Caballes*, 543 U.S. at 408. In this regard, the deployment of Google’s hashing technology is akin to a canine sniff because it is a binary search that “discloses only the presence or absence of [contraband].” *United States v. Place*, 462 U.S. 696, 707 (1983).

⁴ Apparent has a second definition: “seeming real or true, but not necessarily so.” *Pearson*, 810 F.3d at 209. In the context of Google’s statutory obligations, though, apparent is used synonymously with “obvious.” *See* 18 U.S.C. § 2258A(a)(2)(A). It would defy logic for Congress to require Google to report to NCMEC media that is “seemingly [child pornography], but not necessarily so.” Courts must endeavor to avoid “interpretations of a statute which would produce absurd results . . . if alternative interpretations consistent with the legislative purpose are available.” *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982).

In fact, a hash search is significantly more refined: a canine sniff may alert to the presence of narcotics, but it cannot establish the exact type of narcotic, its quantity, or its purity. On the other hand, a hash match between two files establishes that those two files are identical, down to the pixel. *See, e.g.,* Kerr, 119 HARV. L. REV. at 541; Salgado, 119 HARV. L. REV. F. at 46; Martin, 70 STAN. L. REV. at 717; Branham, 53 AKRON L. REV. at 219. If a positive “hit” by a drug-detecting canine justifies government inspection of an item as cavernous (and likely to also hold noncontraband) as a vehicle, *see, e.g., Florida v. Harris*, 568 U.S. 237, 248 (2013); *United States v. Green*, 740 F.3d 275, 282 (4th Cir. 2014); *United States v. Shepard*, No. 7:20-CR-00201, 2021 WL 2160540, at *4 (E.D.N.C. May 27, 2021), it logically follows that a positive “hit” by Google’s hashing technology on an individual file justifies government inspection of that same file.

Most courts to consider the question of whether a government agent’s inspection of a hash value match to child pornography have started from the assumption that the inspection constituted a search subject to the Fourth Amendment, and then proceeded to evaluate whether the government’s search exceeded the scope of the private party’s search. *E.g., Wilson*, 13 F.4th at 967; *Miller*, 982 F.3d at 427; *Reddick*, 900 F.3d at 638. That analytical starting point, in this court’s view, bypasses the critical threshold question of whether the individual seeking suppression maintained a reasonable expectation of privacy in the item that the government searched. The Fourth Amendment safeguards an individual’s right to be free from unreasonable searches and seizures, but it does not protect an individual’s desire to privately possess contraband. *See* U.S. Const. amend. IV; *Katz*, 389 U.S. at 361; *Caballes*, 543 U.S. at 408.

As the *Miller* Court noted, “[c]ourts often must apply the legal rules arising from fixed constitutional rights to new technologies in an evolving world.” *Miller*, 982 F.3d at 417. Fair application of Fourth Amendment law to a technology as “powerful and pervasive,” Salgado, 119

HARV. L. REV. F. at 38, as hashing leads to the conclusion that a government agent's inspection of a hash value match to child pornography does not constitute a search subject to the Fourth Amendment. A hash match to a known image of child pornography represents definitive proof that that matching image is the same image of child pornography. Whether the potential risk of error is one in one billion, Branham, 53 AKRON L. REV. at 219, or one in 9.2 quintillion, *Dunning*, 2015 WL 13736169, at *2, the risk is too slight to suggest any constitutional infirmity in an agent's subsequent inspection of that image. The insignificance of that risk satisfies even the most stringent interpretation of the Fourth Amendment's requirement of reasonableness.

Factually, this case is distinguishable from *Ackerman*, where an internet service provider sent NCMEC a defendant's entire email, which included four attachments, only one of which was identified as a hash value match to child pornography. *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016). Law enforcement then received those materials from NCMEC and reviewed the email, as well as the three attachments that had not previously been identified as child pornography. *See id.*; *see also id.* at 1304 (concluding that NCMEC conducted a search by opening the email). Here, on the other hand, Google only included the 156 images of apparent child pornography in the Report. *See* DE 40-1. Google did not provide NCMEC or law enforcement with access to Defendant's account, which would have been (at least in theory and notwithstanding its limited existence) "capable of storing all sorts of private and personal details, from correspondence to other private (and perfectly legal) images, video or audio files, and beyond." *Ackerman*, 831 F.3d at 1306.

As a consequence, it was virtually impossible that Detective Rider, in inspecting the Report's images and nothing else, would find noncontraband. *E.g.*, *Dunning*, 2015 WL 13736169, at *2; Salgado, 119 HARV. L. REV.; Branham, 53 AKRON L. REV. at 219. To borrow from

Jacobsen, “governmental conduct that can reveal whether [an image] is [child pornography], and no other arguably private fact, compromises no legitimate privacy interest.” *Jacobsen*, 466 U.S. at 123 (internal quotation marks omitted). Because Detective Rider only inspected apparent child pornography, and Defendant has not suggested that the images could have contained anything else, the inspection “d[id] not compromise any legitimate interest in privacy [and was] not a search subject to the Fourth Amendment.” *Caballes*, 543 U.S. at 408. For this reason too, the motion to suppress must be denied.

Third, even assuming Defendant retained a reasonable expectation of privacy in the presence of child pornography in his Google account and the images from that account once they were turned over to law enforcement, Detective Rider’s review of those images did not exceed the scope of Google’s search. To recap, the private search doctrine applies when a subsequent government search does not exceed the scope of a prior private search. *See Bonds*, 2021 WL 4782270, at *2. When there is a “virtual certainty” that a government search will identify “nothing ... of significance” that the private search did not already reveal, the government search does not exceed the scope of the private search. *Jacobsen*, 466 U.S. at 119.

Here, Detective Rider’s inspection of the three images did not exceed Google’s prior search. “At some point, Google employees who are trained on the federal definition of child pornography viewed [those 3] images to confirm that they [we]re illegal child pornography before adding them to its child-pornography repository.” *Miller*, 982 F.3d at 429. The images Defendant subsequently uploaded matched hash values in Google’s repository, meaning those images were the same images that Google employees had already reviewed. *See Salgado*, 119 HARV. L. REV. F. at 40 (“if an unknown file has a hash value identical to that of another known file, then you know that the first file is the same as the second”). Ultimately, then, the inquiry “turns on the

question whether Google’s hash-value matching is sufficiently reliable.” *Id.* at 429-30. Defendant has not contested the reliability of Google’s hashing technology, and, as the court has explained throughout this order, it is exceedingly reliable. *See Dunning*, 2015 WL 13736169, at *2; *accord Wellman*, 663 F.3d at 226 n.2.

As a result, Detective Rider’s search did not exceed Google’s search because there was a virtual certainty that she would identify nothing of significance that Google had not already identified. *See Jacobsen*, 466 U.S. at 119. Google inspected the images, first through human review, and then by means of its hashing technology. Those two layers of review identified the images as apparent child pornography. Detective Rider’s subsequent search replicated and “merely confirmed” the conclusion of the private search. *Reddick*, 900 F.3d at 639.

The motion to suppress urges the court to adopt the Ninth Circuit’s reasoning in *Wilson*, but the court is unpersuaded. The *Wilson* Court held that a law enforcement officer’s inspection of hash match images was a search subject to the Fourth Amendment because that search “substantively expanded the information available to law enforcement far beyond what the label [attached to an image] alone conveyed.” *Wilson*, 13 F.4th at 973. That conclusion misapplies *Jacobsen*, insofar as *Jacobsen* instructs courts to consider whether the subsequent government search reveals something of “significance” that the private search had not already revealed. *Jacobsen*, 466 U.S. at 118. Something of significance, in that context, refers to a noncontraband personal effect in which an individual could have a reasonable expectation of privacy. *See id.* at 118-19 (explaining that box searched by government agent contained only “a tube containing plastic bags” and “white powder” inside of those bags, and so therefore that “a manual inspection of the tube and its contents would not tell [the agent] anything more than he already had been told”); *see also id.* at 120 n.17 (“the precise character of the white powder’s visibility to the naked

eye is far less significant than the facts that the container could no longer support any expectation of privacy, and that it was virtually certain that it contained nothing but contraband”).

Likewise here, Detective Rider’s visual inspection of an image identified by hash value as child pornography could reveal nothing of Fourth Amendment significance because that inspection would only confirm that the image contained child pornography. On some level, the inspection could reveal more information about the specific images (for instance, the particular sex act captured in the image or the number of individuals), which would then enable Detective Rider to describe the image more accurately than using the label provided by Google alone. However, “[p]rotecting the risk of misdescription hardly enhances any legitimate privacy interest, and is not protected by the Fourth Amendment.” *Jacobsen*, 466 U.S. at 119; *see also United States v. Phillips*, 32 F.4th 865, 870 (9th Cir. 2022) (“The only advantage gained by the government’s own search is avoiding the private party’s ‘misdescription’—and that is a permissible advantage.”), *cert. denied*, 143 S. Ct. 467 (2022); *United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990) (holding that government search did not exceed scope of private search “for Fourth Amendment purposes simply because [government agents] took more time and were more thorough than the [private party]”); *United States v. Montijo*, No. 2:21-CR-75, 2022 WL 93535, at *5 (M.D. Fla. Jan. 10, 2022) (concluding that officer’s review of video identified as child pornography did not enable him to “learn new, critical information about the unlawful content” because that review merely allowed him to be “more thorough in describing the illicit material . . . , and his thoroughness does not violate the Fourth Amendment”).

In other words, Detective Rider’s inspection could not reveal anything of significance (within the meaning of *Jacobsen*) because that inspection could only reveal additional information about an item of contraband; the inspection would reveal nothing about any noncontraband. *See*

id. at 118. Because an individual does not have a reasonable expectation of privacy in contraband, *see Caballes*, 543 U.S. at 408, an inspection that only divulges more information about that contraband is not a search subject to the Fourth Amendment.⁵ For these reasons, the visual inspection of the three hash value match images did not exceed Google's search. Therefore, assuming Defendant retained a reasonable expectation of privacy in those images, the private search doctrine applies and warrants denial of the motion to suppress.⁶

⁵ For the same reason, this case is not like *Walter v. United States*, because there the government agent, who received from a private party a box of films that bore labels suggesting the films contained obscenity, "could only draw inferences about what was on the films." *Walter v. United States*, 447 U.S. 649, 650 (1980). No human had reviewed the films before the agent did so in *Walter*. Here, a Google employee had reviewed the images that later matched the hash values of the images Defendant uploaded. The scope and quality of the private party's search in *Walter* bears no resemblance to the scope and quality of Google's search here.

⁶ The motion to suppress would fare no better if the court instead analyzed its claim under a trespass theory. *See* DE 40 at 8-11 (contending that "the law enforcement action also violated [Defendant's] property interests in the folders or files and other contents of the Google Drive account"). The Supreme Court in *Jones* somewhat recently reminded that, irrespective of *Katz*'s reasonable expectation of privacy test, a government agent's "**physical intrusion** of a constitutionally protected area in order to obtain information . . . may constitute a violation of the Fourth Amendment." *United States v. Jones*, 565 U.S. 400, 407 (2012) (emphasis added). Applying a trespass theory to Detective Rider's review of digital files would seriously "strain[] the language of the Fourth Amendment" and be "highly artificial." *Id.* at 419 (Alito, J., concurring in the judgment); *see also id.* at n.2 (noting that "[a]t common law, a suit for trespass to chattels . . . [required] some actual damage to the chattel before the action can be maintained"); *but see eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069 (N.D. Cal. 2000) (finding that "electronic signals sent by [defendant] to retrieve information from [plaintiff's] computer system [were] sufficiently tangible to support a trespass cause of action"). But, even if the court did apply such a theory, Defendant would not be entitled to suppression of evidence because, to the extent any party committed a "trespass," that party was Google. *See Miller*, 982 F.3d at 433 ("if Google's hash-value matching is akin to a party 'opening' a letter, Google might be the one that engaged in the trespass"). Even under a physical trespass theory, a private party's seizure of an individual's personal effects and subsequent transmission of those effects to the government does not prevent the government from using those materials in a prosecution. *See Burdeau*, 256 U.S. at 475 (holding that when "no official of the federal government had anything to do with the wrongful seizure of the petitioner's property, . . . there was no invasion of the security afforded by the Fourth Amendment against unreasonable search and seizure, as whatever wrong was done was the act of individuals in taking the property of another"); *accord Phillips*, 32 F.4th at 874 (explaining that "law enforcement officers do not violate the Fourth Amendment when . . . they mimic the trespass a private individual visited on another's possessions after being alerted to the information uncovered pursuant to that trespass").

The motion to suppress also suggests that the private search doctrine should not apply because Detective Rider received the Report from NCMEC, a purported government agent, and not "directly [from] Google." DE 40 at 16. Defendant does not meaningfully develop an argument in support of this position, and it is unpersuasive. To reiterate, application of the private search doctrine asks courts to consider whether a government search revealed information with regard to "which the defendant's expectation of privacy ha[d] not already been frustrated." *Reddick*, 900 F.3d at 638. The movement of the Report from Google to NCMEC to Detective Rider cannot be said to have resurrected Defendant's expectation of privacy in the images contained within the Report. In addition, Defendant's interpretation of the private search doctrine would have profound practical consequences. For example, the relevant statutory scheme would be rendered meaningless because private internet service providers like Google are required to send reports of child pornography to NCMEC, *see* 18 U.S.C. § 2258A(a)(1)(B), and NCMEC lacks authority to prosecute violations of the federal child pornography laws. Moreover, under Defendant's theory, the private search doctrine in

Fourth, even if the private search doctrine did not apply, and therefore assuming an unreasonable search occurred, the good faith exception would excuse the search. Defendant contends that the good faith exception only applies when “an officer is relying on an issued warrant.” DE 55 at 4; *see also* DE 40 at 16-17. Not so. The exception applies “across a range of cases,” *Davis v. United States*, 564 U.S. 229, 238 (2011), including in circumstances where a government agent acts in reasonable reliance upon on a statute that authorizes the search, *Krull*, 480 U.S. at 358.

Here, Detective Rider “acted in objectively reasonable reliance on a statutory scheme when [he] inspected the [three images].” *Ackerman*, 804 F. App’x at 904. As detailed previously, although Google is under no obligation to monitor user activity, once Google obtains actual knowledge of the presence of child pornography, it is required to make a report to NCMEC. *See* 18 U.S.C. § 2258A(a)(1). NCMEC, in turn, “shall make *available*” those reports to law enforcement. 18 U.S.C. § 2258A(c) (emphasis added).⁷ This statutorily mandated information flow ultimately reached Detective Rider. *See* DE 40-1. By inspecting the images in the Report, Detective Rider merely relied on Google and NCMEC’s compliance with their “statutory reporting requirements.” *Brillhart*, 2023 WL 3304278, at *8. Doing so was objectively reasonable, and the motion to suppress makes no argument to the contrary.

most other circumstances would become a nullity unless the private party conducted a search and then had the prescience to provide the evidence of criminality to the specific government entity or agent tasked with investigating such criminality (consider for example, a private party who finds evidence of terroristic activities on an acquaintance’s computer and then provides that evidence to local law enforcement, who in turn shares the information with the FBI). Ultimately, the private search doctrine turns on “the scope of the antecedent private search,” *Jacobsen*, 466 U.S. at 116, not how many hands the fruits of that search passed through before the subsequent government search. Because Defendant’s version of the private search doctrine would thwart legitimate coordination by law enforcement agencies and would not further any legitimate privacy interest, its application is unwarranted.

⁷ The Report could hardly be considered “available” to law enforcement if Detective Rider could only review its contents after obtaining a search warrant.

“Police practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield meaningful deterrence, and culpable enough to be worth the price paid by the justice system.” *Davis*, 564 U.S. at 240 (cleaned up). Detective Rider’s conduct in this case does not trigger that harsh sanction. Accordingly, the good faith exception applies and requires denial of the motion to suppress.

Fifth, and finally, even if an unlawful search occurred and the good faith exception did not apply, significant intervening events would render that search too attenuated to justify suppression of evidence that law enforcement later obtained. In the present case, the inspection of the three images occurred in May 2020. Months then passed. Law enforcement obtained a search warrant for Defendant’s parent’s home in October 2020. That search did not result in the recovery of any contraband. Defendant’s parents, however, did inform law enforcement that Defendant had moved out months prior and relocated to Raleigh.

Chesapeake PD then closed its investigation, and a new one commenced in North Carolina. Defendant then agreed, in November 2020 (over six months after Detective Rider’s search), to submit to a voluntary interview. At the conclusion of that interview, Defendant provided consent for law enforcement to analyze his personal devices. That analysis revealed the presence of child pornography. When confronted with that evidence, in December 2020, Defendant admitted to transporting a flash drive of child pornography from Virginia to North Carolina. A search of Defendant’s apartment, authorized by a warrant, led to the recovery of that flash drive (as well as a hard drive containing additional contraband). Defendant was then indicted in connection with his transportation and possession of child pornography. His charges do not arise from evidence uncovered during the search in May 2020.

There is no bright-line rule for application of the attenuation doctrine. *See Nardone*, 308 U.S. at 341. The court must consider whether the challenged evidence (i.e., the child pornography recovered on December 8, 2020, and Defendant’s admission on that same day that he transported the child pornography from Virginia to North Carolina), “has been come at by exploitation of [the May 2020 search] or instead by means sufficiently distinguishable to be purged of the primary taint.” *Wong Sun*, 371 U.S. at 488. That test is met here.

Every factor identified in *Brown* favors a finding of attenuation in this case. *See Brown*, 422 U.S. at 603–04. First, the time that passed between any assumed illegality and later-obtained evidence is significant: seven months. Considering that Defendant had no knowledge of the May 2020 search, and that the passage of time is most relevant to the extent it can ameliorate the coercive effect of some illegal government conduct on a criminal suspect, *see Brown*, 422 U.S. at 604; *Wong Sun*, 371 U.S. at 491; *United States v. Owen*, 492 F.2d 1100, 1107 (5th Cir. 1974), the court finds that the amount of time that passed here is substantial and weighs in favor of attenuation.

Second, there were significant intervening circumstances. Defendant’s parents informed law enforcement that Defendant moved to Raleigh and provided them with his phone number and new address. Defendant agreed to submit to a voluntary interview. He consented to a forensic analysis of his devices. He later admitted to possessing and transporting child pornography. And a search at his apartment pursuant to a warrant resulted in the recovery of the evidence which forms the basis of his federal indictment.

Suffice it to say that “police discover[ed] the evidence [in this case] from [multiple] source[s] independent from the illegal conduct.” *Harris*, 1999 WL 133134 at *2. Defendant’s “voluntary consent,” both to submit to two interviews and to permit law enforcement to inspect

his phone and laptop, “is the quintessential act of free will.” *Seidman*, 156 F.3d at 549 n.10. And his confession when confronted with incriminating evidence, which occurred seven months after Detective Rider’s search, was “so attenuated as to dissipate the taint.” *Wong Sun*, 371 U.S. at 491 (finding that voluntary confession *four days* after illegal arrest “was not the fruit of that arrest”); *see also Seidman*, 156 F.3d at 549 (concluding that defendant’s voluntary conversation with law enforcement mere minutes after they illegally entered his home was “independent act[] of free will”).

Lastly, “the purpose and flagrancy of the official misconduct” supports a finding of attenuation. *Brown*, 422 U.S. at 604. Purpose in this context means more than a general law enforcement purpose; it means that the purpose of the conduct was to coerce an individual into providing incriminating evidence. *See id.*; *see also U. S. ex rel. Gockley v. Myers*, 450 F.2d 232, 236 (3d Cir. 1971); *United States v. Edmons*, 432 F.2d 577, 584 (2d Cir. 1970); *accord Utah v. Strieff*, 579 U.S. 232, 241 (2016) (“The third factor of the attenuation doctrine . . . favor[s] exclusion only when the police misconduct is most in need of deterrence.”). Detective Rider never contacted Defendant, and her purpose in viewing those images can only be described as a general law enforcement purpose.

Neither was Detective Rider’s conduct flagrant. Defendant acknowledges that, if Detective Rider had instead viewed images from among the 31 images that the Google employee had inspected prior to generation of the Report, the entire basis for the motion to suppress would be undermined. *See* DE 40 at 13-14 (describing as “[c]rucial” that Detective Rider viewed “three further files” beyond what Google employee viewed). With that in mind, Detective Rider’s inspection of three hash-match images, instead of images reviewed by a Google employee immediately prior to generation of the Report, appears to have been an arbitrary decision which

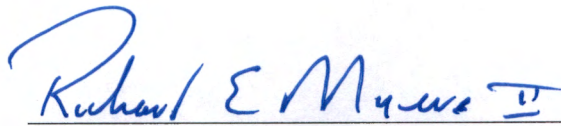
does not connote any sort of flagrant misconduct. Assuming the review of those images impermissibly exceeded the scope of Google’s search, that review was a “mistake” that reflected justifiable “ignorance of the law,” because in these circumstances there is no “well-established warrant requirement set forth by the Supreme Court.” *United States v. Terry*, 909 F.3d 716, 722 (4th Cir. 2018).

In sum, all the *Brown* factors favor attenuation, and the court therefore concludes that any “causal connection between information obtained through [Detective Rider’s search] and the Government’s proof . . . [have] become so attenuated as to dissipate the taint.” *Nardone*, 308 U.S. at 341. That finding merits denial of the motion to suppress.

IV. Conclusion

For the reasons articulated above, the motion to suppress [DE 40] is DENIED.

SO ORDERED this 5th day of February, 2024.



RICHARD E. MYERS II
CHIEF UNITED STATES DISTRICT JUDGE